

## CLAIMS

What is claimed is:

1. A method for a first device and a second device to maintain synchronization of a shared, dynamic secret, the method comprising:
  - the second device sending an authentication request to the first device;
  - the first device, in response to the authentication request,
    - authenticating the second device,
    - sending an authentication reply to the second device, and
    - advancing a first copy of the secret;
  - the second device, in response to the authentication reply,
    - advancing a second copy of the secret;
  - the first device,
    - sending data to the second device,
    - again advancing the first copy of the secret, and
    - sending a data completion message to the second device;
  - the second device,
    - consuming the data, and
    - in response to the data completion message, again advancing the second copy of the secret.
2. The method of claim 1 wherein the first device comprises a server and the second device comprises a web appliance.
3. The method of claim 1 further comprising:
  - the first device storing the again advanced first copy of the secret; and
  - the second device storing the again advanced second copy of the secret.
4. The method of claim 1 further comprising:
  - executing a recovery technique in response to the first and second copies of the secret becoming out of synchronization.

- 1 5. A system for use on a network, the system comprising:  
2 a server including,  
3 a communication interface,  
4 a processor for performing logic operations,  
5 storage,  
6 stored in the storage, a first copy of a secret,  
7 a secret validator, and  
8 means for advancing the first copy of the secret;  
9 a web appliance including,  
10 a communication interface coupling the web appliance to the server over the network,  
11 a processor for performing logic operations,  
12 storage,  
13 stored in the storage of the web appliance, a second copy of the secret,  
14 means for advancing the second copy of the secret; and  
15 the server and the web appliance further including,  
16 a protocol for recovering synchronization of the first and second copies of the secret.
- 1 6. The system of claim 5 wherein the secret comprises a PIN.
- 2 7. The system of claim 6 wherein the PIN comprises a number of at least 80 bits.
- 3 8. A method for a client device to maintain synchronization of a first copy of a secret stored on  
4 the client device with a second copy of the secret stored on a server device, the method comprising  
5 the client device:  
6 sending an authorization request to the server device;  
7 in response to receiving from the server device an authentication reply,  
8 advancing the first copy of the secret; and  
9 in response to receiving data from the server device,  
10 consuming the data, and  
11 again advancing the first copy of the secret.
- 1 9. The method of claim 8 further comprising the client device:

2 in response to receiving data from the server device,  
3 storing the again advanced first copy of the secret.

1 10. The method of claim 8 further comprising the client device:  
2 in response to not receiving an affirmative authentication reply from the server device,  
3 (a) advancing the first copy of the secret,  
4 (b) sending the advanced first copy of the secret to the server device.

1 11. The method of claim 10 wherein the (a) advancing the first copy of the secret comprises  
2 twice advancing the first copy of the secret.

1 12. A method for a server to authenticate an appliance that is in communication with the server,  
2 the method comprising the server:

3 receiving from the appliance an authentication request;  
4 sending an authentication reply to the appliance;  
5 advancing a first copy of a secret stored on the server;  
6 sending data to the appliance;  
7 sending a data completion message to the appliance;  
8 again advancing the first copy of the secret; and  
9 storing the again advanced first copy of the secret on the server.

10 13. The method of claim 12 wherein the secret is a PIN.

1 14. The method of claim 12 wherein the secret comprises a value of at least 80 bits.

1 15. The method of claim 12 further comprising:  
2 determining that the appliance is not authentic and, responsive to that determination,  
3 logging the authentication request, and  
4 disconnecting communication to the appliance.

1 16. An article of manufacture comprising:  
2 a machine-accessible medium including instructions that, when accessed by a machine, cause  
3 the machine to perform the method of claim 8.

1 17. The article of manufacture of claim 16 further comprising:

instructions that, when accessed by the machine, cause the machine to perform the method of claim 10.

18. An article of manufacture comprising:  
a machine-accessible medium including instructions that, when accessed by a machine, cause the machine to perform the method of claim 12.

19. The article of manufacture of claim 18 further comprising:  
instructions that, when accessed by the machine, cause the machine to perform the method of claim 15.

FOR OFFICIAL USE ONLY